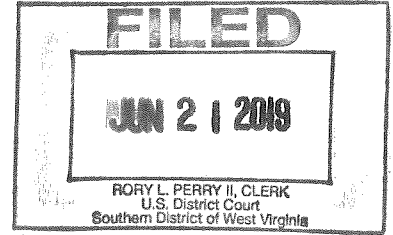


UNITED STATES DISTRICT COURT

for the
Southern District of West Virginia

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

One Apple iPhone, light in color,
bearing IMEI Number 354388065725914

Case No. 2:19-mj-00064

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

One Apple iPhone, light in color, bearing IMEI Number 354388065725914, further described in Attachment A.

located in the Southern District of West Virginia, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252A(a)(2)	Distribution of Child Pornography

The application is based on these facts:

See attached Affidavit.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

First Sgt. Kenneth D. Horrocks, WVSP

Printed name and title

Sworn to before me and signed in my presence.

Date:

June 21, 2019

Judge's signature

City and state: Charleston, West Virginia

Hon. Dwane L. Tinsley, United States Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Kenneth D. Horrocks, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am currently employed as a member of the West Virginia State Police ("WVSP") and have been so-employed since January 2000. My initial training consisted of attending the West Virginia State Police Academy during which I received instruction on various aspects of investigations, including child exploitation, kidnapping, violent crimes and computer intrusions. I am currently assigned to the Oak Hill Detachment and stationed in Beckley, West Virginia. As part of my current assignment, I am responsible for investigating crimes involving the sexual exploitation of children, which are violations of state and federal law. I have participated in the execution of search warrants involving child exploitation, child pornography, and other federal crimes involving the search and seizure of computers and other digital devices related to those offenses. I am currently a deputized member of the West Virginia Internet Crimes against Children Task Force ("WV ICAC") and Homeland Security Investigations ("HSI"), and assist Special Agents with HSI.

2. The statements in this affidavit are based on information provided to me by other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation.

IDENTIFICATION OF THE PROPERTY TO BE EXAMINED

3. The property to be searched is one (1) Apple iPhone, light in color, bearing IMEI Number 354388065725914 (the "Phone"). The Phone is currently located at the WVSP – Oak Hill Detachment, 3057 Main Street, Oak Hill, West Virginia, 25901.

4. In my training and experience, I know that the Phone has been stored in a manner in which its contents are, to the extent material to the investigation, in substantially the same state as it was when the Phone first came into the custody of the West Virginia State Police (“WVSP”). It came into the WVSP’s possession in the following way: The Phone was recovered pursuant to a search incident to a lawful arrest of Daniel Runion by the United States Marshals Service. The Phone is described with particularity in Attachment A.

5. The applied-for warrant authorizes the forensic examination and review of the Phone and its contents for the purpose of identifying electronically stored data as described in Attachment B.

STATUTORY AUTHORITY

6. This investigation concerns alleged violations of 18 U.S.C. § 2252A(a)(2).

That statute provides in pertinent part:

§ 2252A. Distribution of Child Pornography

Whoever—

(1) knowingly mails, or transports or ships using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography;

(2) knowingly receives or distributes--

(A) any child pornography using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; or

(B) any material that contains child pornography using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer[.]

DEFINITIONS

7. The following definitions apply to this Affidavit and its attachments:

a. **Wireless Telephone / Mobile Phone:** A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. **Internet:** The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. **IP Address:** An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers,

each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

d. “**Chat**,” as used herein, refers to any kind of text communication over the Internet or cellular telephone network that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

e. “**Computer**,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

f. “**Computer hardware**,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and

connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

g. **“Computer software,”** as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. **“Computer passwords and data security devices,”** as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

i. **“File Transfer Protocol” (“FTP”),** as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

j. **“Mobile applications,”** as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

k. **“Records,” “documents,” and “materials,”** as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

l. **“Cloud-based storage service,”** as used herein, refers to a publicly accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an Internet connection.

m. **Digital camera:** A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

n. **Portable media player:** A portable media player (or "MPS Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some

portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

o. The term “**minor**,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

p. The term “**sexually explicit conduct**,” 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic areas of any person.

q. The term “**visual depiction**,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disk or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

r. The term “**child pornography**,” as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means of sexually explicit conduct, where:

- i. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

- ii. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
- iii. such visual depiction has been created, adapted or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

8. Based on my training, experience, and research, and from consulting the manufacturer's product manual and technical specifications available online at <https://support.apple.com>. I know that the Phone is a mobile device that has capabilities allowing it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA.

9. In my training and experience, examining data stored on devices of this type can reveal, among other things, who possessed or used the device.

BACKGROUND REGARDING TECHNOLOGY, COMPUTERS AND THE INTERNET

10. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I know the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). Darkroom facilities and a significant amount of skill were required in order to develop and reproduce the photographic images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their detection by the public. The distribution of these

wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Child pornographers can now transfer photographs from a camera in a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem.¹ Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., “Instant Messaging”), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials among pornographers.

¹ The File Transfer Protocol (“FTP”) is a protocol that defines how files are transferred from one computer to another. One example, known as “anonymous FTP,” allows users who do not have a login name or password to access certain files from another computer, and copy those files to their own computer.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has increased tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

e. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Inc. and Google, Inc., among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can often be found on the user's computer.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer

user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained on the computer indefinitely until overwritten by other data.

**BACKGROUND ON THE NATIONAL CENTER FOR MISSING AND EXPLOITED
CHILDREN'S CYBERTIPLINE**

11. Based on my training and experience, and publicly-available information, I know that the National Center for Missing and Exploited Children ("NCMEC") is a nonprofit, nongovernmental organization in Alexandria, Virginia, that works with law enforcement on issues related to missing and sexually exploited children. One of the services provided and administered by NCMEC is its CyberTipline, which serves as the national clearinghouse for leads regarding sexual exploitation crimes against children. NCMEC provides resources, services, and technical assistance to families, private industry, law enforcement, victims, and the general public to assist in preventing child abductions, recovering missing children, and providing services to combat child sexual exploitation. NCMEC performs twenty-two core functions, including serving as a clearinghouse for reports relating to child sex trafficking and providing technical assistance to law enforcement and first responders relating to the identification, location and recovery of child trafficking victims. NCMEC has assisted in the recovery of over 200,000 missing children, and received more than twenty million reports of suspected child sexual exploitation on its CyberTipline.

12. In addition to reports from the general public, Title 18, United States Code, Section 2258A requires all providers of an electronic communication service or remote computing service to the public through a facility or means of interstate or foreign commerce, to report "apparent

child pornography” to NCMEC via the CyberTipline. Leads are reviewed by specially-trained analysts, who examine and evaluate the reported content, add related information that may be useful to law enforcement, use publicly-available search tools to determine the geographic location of the apparent criminal act, and ultimately provide all of the gathered information to the appropriate law enforcement agency for review and possible investigation. Electronic Service Providers (“ESPs”), other online companies and members of the public often also submit reports to the CyberTipline regarding child sex trafficking, although no federal or state law imposes a requirement comparable to the mandated reporting required for child pornography.

13. The CyberTipline thus receives reports, known as CyberTip Reports, on the following type of criminal conduct: possession, manufacture and distribution of child pornography; online enticement of children for sexual acts; child prostitution; sex tourism involving children; child sexual molestation; unsolicited obscene material sent to a child; misleading domain names; and misleading words or digital images on the Internet.

14. The CyberTip Reports will vary in detail depending on the nature of the report, and which entity submits it. The reports can include information (1) relating to the identity of any individual who appears to have violated federal law by committing or attempting to commit the criminal conduct described above; (2) historical information on when or how a customer or subscriber of an electronic communication service or remote commuting service uploaded, transmitted, or received apparent child pornography; (3) geographical information on the involved individual or website, which may include the IP Address or verified billing address or geographic identifying information, including area code or zip code; (4) any images of apparent child pornography; and (5) the complete communication containing any image of apparent child

pornography. See 18 U.S.C. § 2258A(b). Also, as will be illustrated below, CyberTip Reports can be supplemented and made in connection with other CyberTip Reports.

**CHARACTERISTICS OF PERSONS WHO COLLECT OR TRAFFICK CHILD
PORNOGRAPHY**

15. Your affiant has received training presented at the West Virginia State Police Academy where courses of study included criminal investigations and the sexual exploitation of children. Your affiant has also received education through online and onsite trainings and courses offered through the West Virginia Center for Children's Justice, the Office of Juvenile Justice and Delinquency Prevention, and the WV ICAC Task Force.

16. As a result of the aforementioned knowledge, training and experience, your affiant has learned that the following characteristics are generally found to exist in varying combinations and be true in cases involving offenders who send, cause to be sent, distribute, exhibit, possess, display, transport, manufacture or produce material which depicts minors engaged in sexually explicit conduct. Said material may include, but is not limited to, photographs, negatives, slides, magazines, printed media, motion pictures, video tapes, books and other media stored electronically on computers, digital devices or related digital storage media.

17. Offenders who deal with the above-referenced material depicting minors engaged in sexually explicit conduct obtain or traffic in such materials through many sources and by several methods and means. These sources, methods and means include, but are not limited to, the following:

- a. Downloading via the Internet and other computer networks (including from websites, peer-to-peer file sharing networks, news groups, electronic bulletin boards, chat rooms, instant message conversations, internet relay chats, email).

b. Receipt from commercial sources within and outside of the United States through shipments, deliveries and electronic transfer.

c. Trading with other persons with similar interests through electronic transfer, shipments or deliveries.

18. These offenders collect materials depicting minors engaged in sexually explicit conduct for many reasons. These reasons include the following:

a. For sexual arousal and sexual gratification.

b. To facilitate sexual fantasies in the same manner that other persons utilize adult pornography.

c. As a medium of exchange in return for new images and video depicting minors engaged in sexually explicit conduct.

19. These offenders often view their child pornographic materials as valuable commodities, sometimes even regarding them as prized collections. Subsequently, these offenders prefer not to be without their child pornographic material for any prolonged period of time and often go to great lengths to conceal and protect their illicit collections from discovery, theft or damage. To safeguard their illicit materials, these offenders may employ the following methods:

a. The use of Internet-based data storage services.

b. The use of labels containing false, misleading or no title.

c. The application of technologies, software and other electronic means such as encryption, steganography, partitioned hard drives, and misleading or purposefully-disguised applications on electronic devices.

d. The use of safes, safety deposit boxes or other locked or concealed compartments within premises or structures that the offender has control of.

PROBABLE CAUSE

20. Your affiant has learned that on or about March 28, 2019, the WVSP received a Cybertip from NCMEC, which had in turn received its Cybertip from Facebook. This Cybertip indicated that on or about January 30, 2019, a Facebook user utilizing the username Daniel Runion, distributed a video of an unknown male engaged in sexual intercourse with an unknown female. The female in the video appeared to be under the age of ten. Runion distributed the video to a Facebook account bearing the username Cathrine Lynn Marie Cantrell.

21. Further research on or about March 28, 2019, by your affiant determined that the user Daniel Runion was assigned a Facebook User ID of 100027406612017 and was utilizing IP Address 173.80.118.13.

22. Additional research on or about March 28, 2019, by your affiant determined that the user Cathrine Lynn Marie Cantrell was assigned a Facebook User ID of 1000092864863 and utilized IP Address 68.118.77.151. Further research into Cantrell's IP address developed results relating to Lincoln City, Oregon.

23. Your affiant determined that IP Address 173.80.118.13 was associated with Suddenlink Communications. Your affiant subsequently sent an administrative subpoena to Suddenlink Communication for subscriber information regarding IP Address 173.80.118.13. Records returned on or about April 8, 2019, from Suddenlink indicated that the IP address was assigned to Sherry Runion with a physical address of 4157 Seng Creek Road in Whitesville, West Virginia.

24. On or about April 8, 2019, an address search for 4157 Seng Creek Road in Whitesville, West Virginia revealed that Daniel Runion and Crawford Runion had both utilized that mailing address.

25. Your affiant learned that on or about April 26, 2019, West Virginia State Police spoke with an unknown female at 4157 Seng Creek Road in Whitesville, West Virginia who confirmed that Daniel Runion resides in a camper located on the property, behind the residential structure designated as 4157 Seng Creek Road. Pursuant to that conversation, WVSP Troopers took photographs of the 4157 Seng Creek Road residential structure as well as the camper behind it.

26. Your affiant further conducted a criminal history search on Daniel Runion. Your affiant learned that in 2012, in the United States District Court for the Southern District of West Virginia, Daniel Runion was convicted of Receiving Child Pornography in violation of 18 U.S.C. § 2252A(a)(2) and 18 U.S.C. § 2252A(b)(1). Your affiant learned that in 2012, Daniel Runion was sentenced to ninety-seven months of imprisonment with fifteen years of Supervised Release to follow. Your affiant also learned that Daniel Runion is on the West Virginia sex offender registry.

27. In the 2012 case, Daniel Runion used his computer and a file sharing program to knowingly receive images of minors engaged in sexually explicit conduct, including actual or simulated sexual intercourse as well as the exhibition of actual genitalia and pubic regions of the minors. The images and videos were transported using the Internet. At the time, Daniel Runion amassed over 600 images and videos of child pornography on his computer.

28. Your affiant learned that as a result of the 2012 case, Daniel Runion is still on supervised release. Your affiant spoke with the Federal Probation Officer who is supervising Daniel Runion on his Supervised Release. That officer advised that Daniel Runion has been on supervised release since October 2018.

29. On or about April 30, 2019, a state search warrant was issued for the residential structure and the camper located at 4157 Seng Creek Road in Whitesville, West Virginia.

30. On the same date, WVSP executed the search warrant for the residential structure and the camper located at 4157 Seng Creek Road in Whitesville, West Virginia. Upon arrival to the property, a female adult named Cristy Sue Dunlap (“Dunlap”) met the troopers and informed them that she was Daniel Runion’s live-in-girlfriend. Dunlap stated that Daniel Runion was away at work for an Elkview, West Virginia paving company and she was unsure when he would be home that day. Dunlap agreed to message Daniel Runion using the Facebook Messenger Application to ask him when he would be home. Your affiant observed the screen of Dunlap’s phone as she messaged Daniel Runion and specifically observed that Daniel Runion’s Facebook screen name was listed as “Danny Runion.” Daniel Runion did not immediately respond to Dunlap’s inquiry.

31. Troopers advised Dunlap of the search warrant and began searching the interior of the camper. Troopers recovered the following items from within the camper:

- a. 1 HP laptop computer;
- b. 2 Sandisk jump drives;
- c. 1 Samsung camera;
- d. 1 Sandisk card reader;
- e. 4 SD cards;
- f. 1 jump drive wrapped in pink post note labelled blank;
- g. 1 GoPro “HERO” camera;
- h. 3 SD cards;
- i. 1 Seagate external hard drive;
- j. 1 Brix Pro ultra-compact PC kit; and
- k. 1 Smith and Wesson .38 Special Airweight handgun.

The above-listed items were recovered by WVSP Troopers, then secured and photographed. The items were transported to the Oak Hill Detachment and placed into evidence.

32. On this same date, your affiant spoke with Crawford Runion, who is the father of Daniel Runion. Crawford Runion was located on the premises of 4157 Seng Creek Road in Whitesville, West Virginia, as Troopers executed the search warrant on the residential structure. Also present was Sherry Runion, who identified herself as the mother of Daniel Runion.

33. Troopers recovered the following items from within the residential structure located at 4157 Seng Creek Road in Whitesville, West Virginia:

- a. 1 Samsung cellular phone;
- b. 1 black ZTE smart phone; and
- c. 1 NextBook-Intel notebook computer.

34. The above-listed items were recovered by WVSP Troopers, then secured and photographed. The items were transported to the Oak Hill Detachment and placed into evidence.

35. As Troopers searched the residential structure, a contact named "Danny" called Crawford Runion's landline. Sherry Runion answered the call and had a brief conversation with the person on the other end of the phone. Your affiant inquired whether that caller was Daniel Runion and Sherry Runion confirmed that it was Daniel Runion. According to Sherry Runion, Daniel Runion had called to inquire what was going on at the house after hearing there were Troopers present.

36. On that same date, April 30, 2019, your affiant contacted cellular phone number 304-993-7841. Daniel Runion answered the phone and stated that he was leaving his job site in Elkview, West Virginia, and that he would be at the Seng Creek Road address in a little over an hour.

37. Troopers obtained a recorded audio statement from Crawford Runion, who told them that Daniel Runion resides with his girlfriend, Dunlap, in the camper next to his residence at 4157 Seng Creek Road in Whitesville, West Virginia. Crawford Runion stated that Daniel Runion owns the camper and has resided in it on the property for approximately three months. Crawford Runion confirmed that he has Suddenlink internet service and that the internet is password protected. Crawford Runion stated that Daniel Runion has accessed the internet from his camper since approximately November 2018. Crawford Runion provided your affiant with a cell phone number for Daniel Runion of 304-993-7841. Crawford Runion also indicated that Daniel Runion does have access to his residence and he is unsure if Daniel has accessed any of the devices that Troopers located and seized within that residence.

38. Troopers also obtained a recorded audio statement from Dunlap, who stated that she and Daniel Runion met through a social website called "Fetlife" on or about August 1, 2018. Dunlap told officers that Daniel Runion soon thereafter opened a Facebook account under his name and they began communicating through the Facebook Messenger Application. Dunlap stated that Daniel Runion told her he was in prison because he had engaged in sexual intercourse with a girl who he later learned to be either fifteen or sixteen years old.

39. Dunlap informed investigators that she and Daniel Runion moved into the camper in November 2018, and that it was previously parked elsewhere in the yard of 4157 Seng Creek Road in Whitesville, West Virginia. Dunlap stated they had recently moved it to its current location adjacent to the residential structure on the same property.

40. Dunlap also told Troopers that she and Daniel Runion obtained their Wi-Fi from the Suddenlink account belonging to Crawford Runion. She stated that Daniel currently had a Straight Talk mobile phone with internet capability and provided a specific phone number that she

indicated belonged to him. She stated that Daniel Runion's Straight Talk telephone contract was under an alias, but she could not recall the specific name.

41. Dunlap also stated that Daniel Runion had created a new Facebook account with the name "Danny Runion" because his old Facebook account was disabled.

42. Dunlap further stated that the Smith and Wesson .38 Special Airweight Revolver handgun ("firearm") that WVSP Troopers recovered from within the camper was hers but that Daniel Runion possessed and carried this firearm on several occasions. Dunlap claimed that she had previously spoken to Daniel Runion about carrying the firearm because she knew if he got caught with the firearm, he would likely return to prison. Dunlap stated that when she reminded Daniel Runion of this, he normally apologized and placed the firearm back in the camper. Dunlap stated that Daniel Runion was the person who placed the firearm in the location wherein WVSP Troopers located it during their search.

43. On that same date, April 30, 2019, around 8:45 p.m., Daniel Runion returned to the Seng Creek Road property from his work in Elkview, West Virginia. Your affiant spoke with Daniel Runion and advised him of circumstances surrounding the investigation. Troopers provided Daniel Runion with *Miranda* warnings and DPS Form 79. Upon receiving such, Daniel Runion agreed to provide your affiant with an audio statement which was recorded.

44. In his recorded audio statement, Daniel Runion stated that he did recall communicating with Cathrine Lynn Marie Cantrell on Facebook, however, he did not recall what was contained in the video he sent to her. Daniel Runion stated that he and Cathrine Lynn Marie Cantrell distributed several videos to one another. Daniel Runion acknowledged that he once had a Facebook account under the name "Daniel Runion" and estimated that he started the Facebook account on or around the beginning of January 2019. Daniel Runion stated that the "Daniel

Runion” Facebook account was eventually disabled so he created a new profile under the name “Danny Runion.” Daniel Runion estimated that he started this account sometime around the first half of February 2019. Daniel Runion stated that he never gave anyone else access to his accounts, and if a video was sent from one of the Facebook accounts, it was sent by him.

45. Daniel Runion stated that at the time of his Facebook communications with Cathrine Lynn Marie Cantrell, he was utilizing the Wi-Fi from the nearby residence of his father, Crawford Runion.

46. Daniel Runion stated that he knew there was a firearm in the camper, however it belonged to his girlfriend, who he identified as Cristy Sue Dunlap. Daniel Runion stated that the firearm should have been in his girlfriend’s truck.

47. Daniel Runion also acknowledged that he had possession of the smartphone that was linked to the number 304-993-7841 provided by Dunlap and Crawford Runion to WVSP Troopers. He stated that when he found out law enforcement officers were at his residence, he threw it in the river because he knew it was a violation of his supervised release.

48. On this same date, April 30, 2019, your affiant coordinated with Special Agent B. Morris of the Department of Homeland Security. Your affiant advised SA Morris of the circumstances of this investigation and SA Morris indicated that he would assist as needed.

49. On May 1, 2019, your affiant spoke with Daniel Runion’s supervising Federal Probation Officer, Doug Smith. Your affiant informed Probation Officer Smith of the circumstances of this investigation and provided him with requested information.

50. On this same date, SA Morris contacted your affiant and informed him that DHS had completed a Facebook preservation request for the Facebook accounts of Cristy Sue Dunlap and Daniel Runion’s new Facebook account, “Danny Runion.” SA Morris also indicated that he

had completed an ATF E-trace on the Smith and Wesson .38 firearm recovered from Daniel Runion's camper.

51. On May 2, 2019, Probation Officer Smith contacted your affiant and advised that he had texted Daniel Runion on the 304-993-7841 mobile phone number that he had previously provided to law enforcement investigators during the execution of the search warrant. Probation Officer Smith indicated that Daniel Runion sent him a reply text message which indicated that Daniel Runion possibly still had the mobile phone device that he previously told law enforcement investigators he had thrown into the river.

52. On May 6, 2019, all evidence recovered from the camper and the residential structure was transported by your affiant to the Forensic Laboratory for analysis and testing.

53. On May 8, 2019, the U.S. Marshal's Service arrested Daniel Runion at a hot dog stand in Marmet, West Virginia. There, law enforcement officers who detained Daniel Runion found him to be in possession of an iPhone cellular telephone. This device was seized and secured by the Marshal's Service.

54. An iPhone cellular telephone is a "smart" mobile device that is capable of containing multi-media such as photographs and videos, as well as hosting applications such as Facebook Messenger, an application that Daniel Runion regularly utilized and via which he distributed a video of child pornography.

55. On May 10, 2019, Dunlap voluntarily provided a statement to Special Agent B. Morris of the Department of Homeland Security. Dunlap provided SA Morris with information that Daniel Runion falsely told law enforcement that he threw his phone into the river on the day of the search warrant at his residence. Dunlap described that Daniel Runion returned to his work site to retrieve his cell phone after law enforcement finished searching his residence and departed.

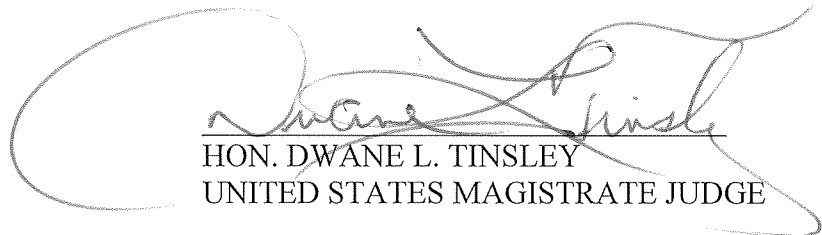
Dunlap described Runion's cell phone as an iPhone, which she described as white. Dunlap also described that Daniel Runion had at least two cell phones – a flip phone he used to communicate with his Probation Officer, and the iPhone that Marshals located during the arrest. She provided law enforcement officers with the passcode to this iPhone.

CONCLUSION

56. Based on the foregoing, there is probable cause to believe that the federal criminal statute cited herein has been violated, and that the contraband, property, evidence, fruits and instrumentalities of the offense, more fully described in Attachment B, are located at the location described in Attachment A. I respectfully request that this Court issue a search warrant authorizing the examination of the Phone described in Attachment A, and authorizing the seizure and search of the items described in Attachment B.


KENNETH D. HORROCKS
First Sergeant, West Virginia State Police

Subscribed and sworn to me this 21st day of June, 2019.


HON. DWANE L. TINSLEY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

ITEM TO BE SEARCHED

1. The property to be searched is one (1) Apple iPhone, light in color, bearing IMEI Number 354388065725914 (the “Phone”). The Phone is currently located at the West Virginia State Police – Oak Hill Detachment, 3057 Main Street, Oak Hill, West Virginia, 25901.

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Section 2252A(a)(2):

1. Phone or storage media used as a means to commit the violations described above.
2. For any Phone or storage medium whose seizure is otherwise authorized by this warrant, and any Phone or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "Phone"):
 - a. evidence of who used, owned, or controlled the Phone at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the Phone, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence indicating how and when the Phone was accessed or used to determine the chronological context of Phone access, use, and events relating to the crimes under investigation and to the Phone user;

- e. evidence of the connection, either physical or via Wifi or Bluetooth, to the Phone of other storage devices or similar containers for electronic evidence;
 - f. evidence of programs (and associated data) that are designed to eliminate data from the Phone;
 - g. evidence of the times the Phone was used;
 - h. passwords, encryption keys, and other access devices that may be necessary to access the Phone;
 - i. records of or information about Internet Protocol addresses used by the Phone;
 - j. records of or information about the Phone's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses revealing an interest in stalking content and/or the identity of the Phone user; and
 - k. Records and information revealing the use and identification of remote computing services, such as email accounts or cloud storage.
3. As used above, the terms "records" and information" include all of the foregoing items of evidence in whatever form and by whatever means they have been created and stored.
4. This warrant authorizes the forensic examination and review of the Phone and its contents for the purpose of identifying the electronically stored information described above.